Amendments to the Specification:

Paragraph beginning on page 7, line 14

Fig. 6 is a block diagram illustrating an example embodiment of a station incorporating transmitter and receiver circuits adapted to perform the ~~acquisition and synchronization mechanisms~~ intrusion and jamming detection mechanism of the present invention; and

Paragraph beginning on page 10, line 18

The mechanism of the present invention uses the concept of an emergency packet that is sent during a special time window referred to as an emergency window that follows the end of each packet. Alternatively, the emergency window can be defined in any other time slot as long as all nodes [[know]] have knowledge of the time slot. Before transmitting, stations listen during the emergency window for the transmission of an emergency packet sent in response to the detection by a victim node of the presence of an imposter node. The emergency packet comprises a special packet that is recognized by all nodes as an emergency packet since it is only transmitted during the emergency window.

Paragraph beginning on page 10, line 24

The function of the emergency packet is to inform the network about the ~~detection~~ presence of an imposter node. An imposter node is defined as a node that illegally transmits a packet utilizing a source address belonging to another node. A victim node is defined as a node that recognizes that an imposter node has transmitted a packet incorporating its own address as the source address of the packet. A receiver node (i.e. destination node) is defined as the node that receives a packet either from the imposter node or from a legitimate node. A carrier signal is defined as a signal modulated in accordance with the particular modulation scheme used to communicate between nodes in the network.

Paragraph beginning on page 11, line 24

In normal operation, the receiver node receives the packet but does not yet know if the packet just received is a legitimate packet or is an imposter packet sent by an imposter node. Before the receiver node sends any acknowledgement or transfers the packet to the upper communication layers for processing, it must make sure the packet is not an imposter packet. This is achieved by listening to the line for carrier signal during the emergency window. If carrier signal is detected during the emergency window, one of the following ~~three~~ four scenarios occurs:

Paragraph beginning on page 12, line 12

3. The carrier signal detected was a false carrier detect and ~~there in actuality~~ there is actually no imposter in the network.
4. The imposter ~~sends~~ transmits noise ~~high~~ large enough to mask the receiver. Note that some type of energy detection means can be used to detect this.

Paragraph beginning on page 13, line 14

If, however, the imposter node jams the reception of the emergency packet (indicated by the dashed arrow 174) but the receive node detects carrier signal during the emergency window, [[its]] it broadcasts an emergency packet request (referenced 176). The victim node hears the EPR message and resends the emergency packet (referenced 178). The imposter may ~~gain~~ again jam the emergency packet message (referenced 180) and the process may repeat a predefined number of times (three [[is]] in the example presented herein). In this case, the receive node transmits the EPR message (referenced 182) ~~gain~~ again and the victim node resends the emergency packet (referenced 184) which is again jammed by the imposter (referenced 186).

Paragraph beginning on page 13, line 25

The present invention also provides for the following exception case whereby the victim node is also the receive node. In other words, the imposter sends a packet to the victim node wherein both the source and destination addresses are the same as that of the victim node. In this case, there is no need to send an emergency packet, since the receive node (i.e. itself) already knows about the imposter. Thus, the victim node immediately transfers the packet to the upper layers with an indication that the packet [[if]] is from an imposter node and that the presence of the imposter is confirmed.

Paragraph beginning on page 13, line 32

Note that in this example, the emergency packet and emergency packet request are broadcast and comprise a regular packet having a control field configured to indicate that the packet is either an emergency packet or an emergency packet request. Alternatively, the emergency packet is not broadcast but transmitted by unicast means as long as the receiver knows the address of the victim. In the case where the message from the imposter was broadcast, the emergency packet is preferably also broadcast. Note that the length of the emergency window is not necessarily equal to the length of the emergency packet ~~packet~~.

Paragraph beginning on page 14, line 5

A flow diagram illustrating the receive packet method of the present invention that is performed upon the end of each packet transmitted on the network is shown in Figures 4A and 4B. This method is performed by each node at ~~the time of~~ the end of the just received packet, before the beginning of the emergency window (i.e. before UST #1). It is typically performed by the data link layer (i.e. MAC layer) within the node.

Paragraph beginning on page 17, line 1

If there was a carrier detect during the emergency window, i.e. the EmergencyCD flag is set due to an attempt by the victim node to send an emergency packet (step 80), no acknowledgement will be sent from any node during the acknowledgement window since the imposter should not be acknowledged. The MustSendACK flag is thus set to false (step 82). The EmergencyCD flag set by the PHY layer is cleared to false (step 84). It is then checked if the node was the receive node, i.e. the previous packet was addressed to it (step 86). All other nodes exit the method.

Paragraph beginning on page 17, line 8

If the node is the receive node (i.e. WeReceivedPacket flag is true) (step 86), the emergency packet counter (EP Counter) is incremented by one (step 88). The node that received the last packet knows that the carrier signal was detected during the emergency window from an emergency packet intended for it. ~~Thus,~~ The node thus suspects that an emergency packet was sent to it but was jammed by the imposter.

Paragraph beginning on page 17, line 27

Thus, to ensure that the network is informed about an imposter the victim node transmits a regular packet to the Network Administrator informing that someone used its address. The regular packet is transmitted after the emergency packet and emergency packet request session. This packet is preferably transmitted as a regular packet since the timing of such a packet is unknown and therefore very difficult to predict by the imposter node.